ARM

In line with my other documents ARA – For the new kid on the block & EAM – For the new kid on the block, this is yet another document to help people who are new to this neck of the woods/Access Control, an overview of my understanding of what ARM is all about and how it works.

As usual feel free to skip it if you are well versed in this topic, however please do stick around and feel free to enlighten me with your expertise if I made any mistakes or if you would like to correct/add more on/to this topic.

Access Request Management (ARM)
Provisioning access to users, in the traditional manner, involves the user completing paper forms that request access to backend systems or business applications. Those forms are then submitted to the first-line approver who reviews, approves, and forward them to second-line approvers who are IT security or the request can be automatically provisioned by the administrator of the target system. Usually, during the approval process, the managers who review access requests are expected to research and identify any potential conflicts of interest between roles that the requester currently has and any new roles including permissions being requested. However, access requests that are under-research and are expedited for approval can cause significant problems where legal, regulatory, security, and financial risks can potentially harm the corporation. ARM automates the access provisioning approval process by linking the request with workflows. When a user (Requester) makes an access request to resources for which they do not have permission or need access to, ARM automatically forwards the access request to designated managers and approvers within a pre-defined workflow. This workflow is customized to reflect your company's policies. Roles and permissions are automatically logged to the enterprise directories when the access requests are approved for future reference and audit purposes. ARM ensures corporate accountability and compliance with Sarbanes-Oxley (SOX) along with other laws and regulations.

Access Request Management (ARM)

The Nitty Gritty

Basic Functionality of ARM

- A Requester initiates a request using the access request page, which is pre-configured by the Administrator
- Upon submission of the Access Request, a workflow gets triggered based on the selection/s in the request
- These selections are linked with conditions that are pre-defined by the admin
- At each approval point (stage), An approver receives a request, which he/she can analyze/run risk analysis/mitigate and based on the findings can choose to approve/reject/hold a request
- Upon approval at all stages the request is automatically provisioned using Auto Provisioning.
- The request and its outcome are logged and can serves as an Audit Trail for security/monitoring/legal purposes.

Auto Provisioning: When the request is raised, the information filled out in the request form is held temporarily and once the request is approved, Auto Provisioning kicks in. So, all this does is create the user/role etc from the request, in the specified system.

Stages of an initiated request

Approving, rejecting, or forwarding a request can involve:

- Selecting a new or a different role for the requester
- Analyzing for SoD risks
- Enforce date/time stamped comments
- Removing offending roles for SoD purposes
- Applying a mitigation control to the pertinent user/role
- Close a request in a variety of ways
- Partial approval (reject some roles and approve the rest)
- E-mail notification when a request is generated, approved, or rejected

Types of users in ARM

- Requester: Any user who can request something for them self or someone else
- Approver: Someone who has got the authority to approve/deny that request
- Administrator: Someone who sets everything up; including Access Request pages,workflows, conditions etc.

Kingpins of ARM

MSMP

Multi Stage Multi Path or simply MSMP is a workflow engine which can be used to accommodate various scenarios of a company's approval and provisioning processes. It is flexible and robust enough to handle user-specific requirements. It can be integrated with other applications/modules like BRF+, Function module, ABAP class, which can be used to define, test and maintain rules that acts as triggers for a specific workflow.

So how does an MSMP workflow work?

- When a requester requests/initiates an action (ex: 'New Account'), it triggers the new account initiator, which is tied up to a specific path that calls upon predetermined stages and these stages have the necessary approvers and settings built in, which dictates how a request should be

Access Request Management (ARM)

The Nitty Gritty

Basic Functionality of ARM

- A Requester initiates a request using the access request page, which is pre-configured by the Administrator
- Upon submission of the Access Request, a workflow gets triggered based on the selection/s in the request
- These selections are linked with conditions that are pre-defined by the admin
- At each approval point (stage), An approver receives a request, which he/she can analyze/run risk analysis/mitigate and based on the findings can choose to approve/reject/hold a request
- Upon approval at all stages the request is automatically provisioned using Auto Provisioning.
- The request and its outcome are logged and can serves as an Audit Trail for security/monitoring/legal purposes.

Auto Provisioning: When the request is raised, the information filled out in the request form is held temporarily and once the request is approved, Auto Provisioning kicks in. So, all this does is create the user/role etc from the request, in the specified system.

handled.

- The request goes through the predefined path and checks off the necessary approvals/rejections. Based on the outcome at each stage it could take a detour, a completely new path (escape route), branch off at the initiator point into two distinct paths (fork route) or branch out at a certain stage into multiple paths (Parallel paths).

**** Fork Route & Parallel paths is more of a 5.3 concept, however the same principle can be used to build conditions to get the desired outcome.***

Workflow Checklist:

- Deciding on specific conditions that should trigger a workflow
- Associating that condition to a Process Id
- Number of levels of approvals (stages)
- Authorized approver for each level (stage)
- Contingency plans for request denials (mitigate, cancel etc).
- Contingency plans if approver/s do not respond within the specified time limit (email reminders, escalation etc)
- Contingency plans if only a part of the request is approved. As in the case of multiple roles with multiple owners (Alternate approver, mitigate etc)
- Auto Provisioning or not in case a request gets approved. If No, then how to proceed?

To make better sense of how MSMP works, please check out this brilliant document put together by Colleen Lee

MSMP – Multi Step Multi Process – GRC's answer to Workflow Configuration Flexibility

and for BRF+, the following document by Shaily Kulshreshtha (Thanks Shaily!):

BRF plus Flate Rule – GRC Integration – Governance, Risk and Compliance – SCN

Access Request Management (ARM)

The Nitty Gritty

Basic Functionality of ARM

- A Requester initiates a request using the access request page, which is pre-configured by the Administrator
- Upon submission of the Access Request, a workflow gets triggered based on the selection/s in the request
- These selections are linked with conditions that are pre-defined by the admin
- At each approval point (stage), An approver receives a request, which he/she can analyze/run risk analysis/mitigate and based on the findings can choose to approve/reject/hold a request
- Upon approval at all stages the request is automatically provisioned using Auto Provisioning.
- The request and its outcome are logged and can serves as an Audit Trail for security/monitoring/legal purposes.

Auto Provisioning: When the request is raised, the information filled out in the request form is held temporarily and once the request is approved, Auto Provisioning kicks in. So, all this does is create the user/role etc from the request, in the specified system.

Wiki

Notifications

Most events from submission of an access request to the close of that request have built in automated notifications that get sent out. These events in the workflow process can trigger an email notification that corresponds to exactly one pre-defined message class. Each message class corresponds to one document object containing a pre-delivered message body for the respective workflow event. The link between message class and pre-delivered document object can be viewed, but not altered in the GRFNVNOTIFYMSG table (SE16).

- You can use either the pre-delivered message bodies, or replace them with customized text messages including notification variables that refer to request attributes, user IDs, and other content.
- In order to replace the pre-delivered standard messages, for a particular workflow event, with customized email notifications; you must perform the following procedures:
    - Create Custom Document Objects: SE61 -> Document Name: ex: Z_GRAC_AR_SUBMIT -> Create -> Enter details
    - Associate Custom Document Object with Message Class: SPRO -> IMG -> Workflows -> Maintain Custom Notification Messages
    - Maintain text/body for the newly created document: SPRO -> IMG -> Workflows -> Maintain Text for Custom Notification Messages
    - Assign them to notification templates in MSMP WF.
- The processes SAP_GRAC_ACCESS_REQUEST and SAP_GRAC_ACCESS_REQUEST_HR are the only workflow processes that come with message template classes for request submissions (GRAC_AR_SUBMIT) and completions (GRAC_AR_CLOSE). You can select them together with their recipients in the section, “Process Global Settings”, in the first step of the MSMP Workflow
- Notification Templates for the events New Work Item, Approved, Rejected, Forward, and Escalation are selected at stage level in step 5, Maintain Paths. Select the stage you want to select notification templates for and

Access Request Management (ARM)

The Nitty Gritty

Basic Functionality of ARM

- A Requester initiates a request using the access request page, which is pre-configured by the Administrator
- Upon submission of the Access Request, a workflow gets triggered based on the selection/s in the request
- These selections are linked with conditions that are pre-defined by the admin
- At each approval point (stage), An approver receives a request, which he/she can analyze/run risk analysis/mitigate and based on the findings can choose to approve/reject/hold a request
- Upon approval at all stages the request is automatically provisioned using Auto Provisioning.
- The request and its outcome are logged and can serves as an Audit Trail for security/monitoring/legal purposes.

Auto Provisioning: When the request is raised, the information filled out in the request form is held temporarily and once the request is approved, Auto Provisioning kicks in. So, all this does is create the user/role etc from the request, in the specified system.

the recipients to receive them and click on Notification Settings

To get a better understanding of how Notification Templates work and to customize them, please check out the following document by Frank Rambo (Thanks Frank!):

AC 10.0 – How to Customize Notification Templates for AC Workflow

Access Request forms & End User Personalization

This is the form a user (requester) uses to raise a request, which triggers the workflow. The Access Request form holds all of the relevant information a user would like to add to the request. The administrator can decide which fields are mandatory, which ones are optional, whats visible and whats editable. Given its importance, it is worth checking out how they can be customized and enforced, so the end user can only access, request forms relevant/tailored for them. A good way to achieve this is by enabling 'template' based access requests and hiding the default 'Access Request' link.

Here are a couple of documents, thanks to Jonathon Pries & Jatin Grover, that are worth checking out.

Creating Access Request: Template Based Requests and Configuring End User Personalization forms for use with AR...

Customizing Access request and approval screens in GRC Access Control

Configuration in a Nutshell

1. Create all ARM users or decide amongst the existing users who gets what ARM role using 'SU01'
2. Create/customize all ARM roles using 'PFCG'
    - SAP_GRAC_MSMP_WF_ADMIN_ALL: Administrator role for MSMP workflows
    - SAP_GRAC_MSMP_WF_CONFIG_ALL: Configuration role for MSMP

Configuration in a Nutshell

workflows
- SAP_GRAC_ACCESS_APPROVER: Approver for Access Request and User Access Review
- SAP_GRAC_CONTROL_APPROVER : Approver for Control Maintenance and Assignments requests
- SAP_GRAC_RISK_OWNER: Approver for Risk Maintenance and SoD Risk Review
- SAP_GRAC_ROLE_MGMT_ROLE_OWNER: Approver for Role Maintenance

3. Assign the roles to their respective users using 'SU01'
4. Add users to user groups using SUGR (To maintain agents – if you choose to use this type of agent)
5. Maintain GRC System Configuration Parameters:
   - SPRO -> IMG -> GRC -> AC-> Maintain Configuration Settings ->
     - Risk Analysis – Access Request
     - Workflow
     - Access Request Role Selection
6. Activate/Check GRC_MSMP_CONFIGURATION BC Set using 'SCPR20'
7. Maintain Connection Settings: 'PROV' Integration scenario
   - SPRO -> IMG -> GRC -> Common Component Settings -> Integration Framework -> Maintain Integration Scenario
8. Maintain Service Level Agreements: This is done to ensure a task is completed within a certain time frame, which will be helpful for generating performance reports and billing external entities
   - SPRO -> IMG -> GRC -> Access Control -> User Provisioning -> Maintain Service Level Agreements
9. Define/Maintain Request Types: You can maintain pre-delivered request types (New/Change/Delete Account etc) and associate a relevant action
   - SPRO -> IMG -> GRC -> Access Control -> User Provisioning -> Define Request Type
10. Maintain Priority Configuration: You can create a priority to establish the urgency of a request
    - SPRO -> IMG -> GRC -> Access Control -> User Provisioning -> Maintain Priority Configuration
11. Define/Maintain Employee Types: you can define the type of Employees (Permanent, Contract, Part time etc)
    - SPRO -> IMG -> GRC -> Access Control -> User Provisioning -> Define Employee Types
12. Define/Maintain Number Range Intervals for Provisioning Requests: Every request made in ARM uses a number to identify the request. A specific range should be given and you got to make sure that ranges don't overlap.
    - SPRO -> IMG -> GRC -> Access Control -> User Provisioning -> Maintain Number Range Intervals for Provisioning Requests or SNRO
13. Maintain End User Personalization: Lets you customize the various attributes (BP, Company, Emp type, Manager etc), which show up on the request page.
    - SPRO -> IMG -> GRC -> Access Control -> User Provisioning ->End User Personalization
14. Maintain Provisioning Settings: This setting collects approvals and then provisions user access to the target systems.
    - SPRO -> IMG -> GRC -> Access Control -> User Provisioning -> Maintain Provisioning Settings.
15. Maintain User Defaults: This is where you can specify certain user defaults based on their geographical location (Date format, time zone etc)

Access Request Management (ARM)

Configuration in a Nutshell

- SPRO -> IMG -> GRC -> Access Control -> User Provisioning ->User Defaults

16. Maintain Review Rejection Reasons: This is where you can specify the reasons why a request is rejected
    - SPRO -> IMG -> GRC -> Access Control -> User Provisioning ->Maintain Review Rejection Reasons
17. Create/Maintain AC Owners
    - NWBC -> Setup -> Access Owners -> Access Control Owners
18. Create/Maintain/Customize/ MSMP Workflows
    - SPRO -> IMG -> GRC -> Access Control -> Workflow for Access Control
        - o Activate Event Linkage for AC Workflows: You maintain the event 'START', which triggers the event for Access Control Workflows for all 10 Process Ids
        - o Maintain MSMP Versions: This is where you maintain/customize MSMP workflows.
        - o Generate MSMP Process Versions: Executing this checks and displays changes made since the activation of the previous version performed in the last step (above)
        - o Define Workflow-Related MSMP Rules: Creates an empty Rule/Shell that can be used to create conditions to trigger a workflow using BRF+, Function module etc
        - o Define Business Rule Framework: This is where you create the conditions to trigger the workflows. This is associated with the empty rule created in the previous step
        - o Create/Maintain Custom Notification Messages: This is where you Create/Maintain custom docu objects that gets sent to end users (Requester, Approver etc)
        - SPRO -> IMG -> GRC -> Access Control -> Workflow for Access Control -> Maintain Custom Notification Messages
        - o Maintain/Customize Text for Custom Notification Messages: This is where you Maintain/Customize the body/text for the docu objects that gets sent to end users
        - SPRO -> IMG -> GRC -> Access Control -> Workflow for Access Control -> Maintain Text for Custom Notification Messages
        - o Maintain Background Job for E-Mail Reminders: This is where you schedule a email reminders background job for MSMP processes like escalation notifications
        - SPRO -> IMG -> GRC -> Access Control -> Workflow for Access Control -> Maintain Background Job for E-Mail Reminders or SM36

Once all of this is done, Create an access request and check if a workflow is getting triggered based on your selections and the conditions you defined. You can check the Instance logs and provisioning logs in NWBC -> Access Management -> Access Request Administration, to get a better understanding of the workflow of a request.

This pretty much is the gist of ARM and should be enough to get you started. For a more comprehensive understanding/configuration and other bits and pieces on this topic, please check out the links in the following document put together by ***Alessandro***, which covers everything in detail. Please check under Access Request Management (ARM).